CTS Mobile Device Management [MDM]

Agency Pre-Implementation Tasks & Decisions

CTS's MDM vendor AirWatch provides a robust solution which leverages Microsoft Active Directory and multi-tenancy which means each agency will manage their own mobile devices and users, including creating groups, and user profiles specific to their agency, but still within the boundaries of OCIO policies on mobile devices. At this time, there is limited information available on specifics of the CTS MDM service; however, even without these details agencies can still begin the process of preparing internally for how they plan on managing the MDM service in their agency. Below is a list of tasks and decisions that each agency will need to have addressed prior to coming on board the CTS MDM service, please review them.

If you have any questions regarding the items below or any general questions about the CTS MDM service, please contact the CTS Service Desk Servicedesk@cts.wa.gov or CTS Mobile Messaging mobilemessaging@cts.wa.gov

1. Develop & define the agency MDM support model/processes.
    a. Identify who will be agency MDM administrators will be that will have access to the agency's section of the AirWatch admin console. E.g. Help Desk staff, Telecom staff, both…
    b. Identify who in the agency is responsible for creating and authorizing MDM policies, rules and groups. Example: Who is authorized to have all agency cameras disabled on State owned mobile devices? The second part of this is again is who actually going to make the changes in the agency AirWatch console?
        i. Agency signing authority for MDM SLA.
        ii. Primary & secondary technical contacts/agency MDM administrators.

2. Is the agency allowing BYOD devices? If so, what are the processes surrounding approval, use and support of BYOD devices?

3. Is the agency allowing or disabling access to the Apple, Google or Windows Stores?

Note: Agencies will have to download the AirWatch MDM client App from one of these 3 public Stores prior to enrolling a device on the AirWatch MDM service, however, once enrolled agency Profiles can be set to disable any further access to the public Stores.

4. Identify any Free or paid Apps that the agency would like to have on all agency devices or identify a subset of users that will have these Apps installed.

5. Develop agency specific Terms of Use screen that each user gets when enrolling mobile devices.

6. Decide what programmable consequences the agency wants to implement if an agency's user's device is 'Jailbreak' e.g. send a customized pop message to device, disable device entirely, turn off email, do nothing, etc…

7. Decide what programmable consequences the agency wants to implement if an agency's user downloads an agency determined unauthorized App e.g. send a customized pop message to device, disable device entirely, turn off email, do nothing, etc…

8. Requirements to access agency AirWatch console - workstation & network requirements, and Active Directory permissions completed.

9. What reporting functionality is the agency anticipating developing? E.g. Last contact time report, wireless carrier data usage by user, all agency users by mobile operating system, etc…

10. How many users is the agency planning on using the CTS MDM service?

11. What percentage of agency users is using Windows8, Android, iOS? Please provide the best estimate possible.

12. Agency policy and procedures when a MDM mobile device is lost or stolen.

13. Agency use of the AirWatch end user self-service portal. What level of functionality to provide end users, or decide not to use it?